

PRÁCTICA 5: Seguridad en redes corporativas

Transmisión de Datos y Redes de Computadores
3º Grado en Ingeniería Informática
Especialidad Tecnologías de la Información

Germán Martínez Maldonado
Pablo Sánchez Robles

1. Configure las tablas de encaminamiento del router al que se conecta directamente para que pueda alcanzar a los otros ordenadores de su isla. No olvide configurar la ruta por defecto de su ordenador para que la pasarela por defecto sea dicho router.

Como nuestro router es el R1_1 (dirección IP interfaz datos: 33.1.1.1), para alcanzar el resto de ordenadores de nuestra isla debemos configurar la tabla de encaminamiento de nuestro router para que sepa cómo llegar a los ordenadores de las redes 33.1.2.0 (mediante el router R1_2) y 33.1.3.0 (mediante el router R1_3), esto lo podemos conseguir indicando que acceda a través de la interfaz de la red interna (eth2) y la dirección de dicha interfaz en ambos routers (172.16.1.2 para el router R1_2 y 172.16.1.3 para el router R1_3). Esta información la podremos introducir mediante WinBox desde el menú IP -> Route -> Botón +. Lo único que falta por añadir es la ruta por defecto en nuestro ordenador que lo podemos hacer introduciendo el comando “route add default gw 33.1.1.1”.

Route <33.1.2.0/24>

General Attributes

Dst. Address: 33.1.2.0/24

Gateway: 172.16.1.2 reachable ether2

Check Gateway: ☐

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

OK Cancel Apply Disable Comment Copy Remove

disabled active static

Una vez configurada la tabla de encaminamiento con las rutas necesarias queda como se ve en la siguiente imagen:

admin@33.1.1.1 (R1_1) - WinBox v4.5 on RB433 (mipsbe)

Interfaces Wireless Bridge PPP Switch Mesh IP MPLS

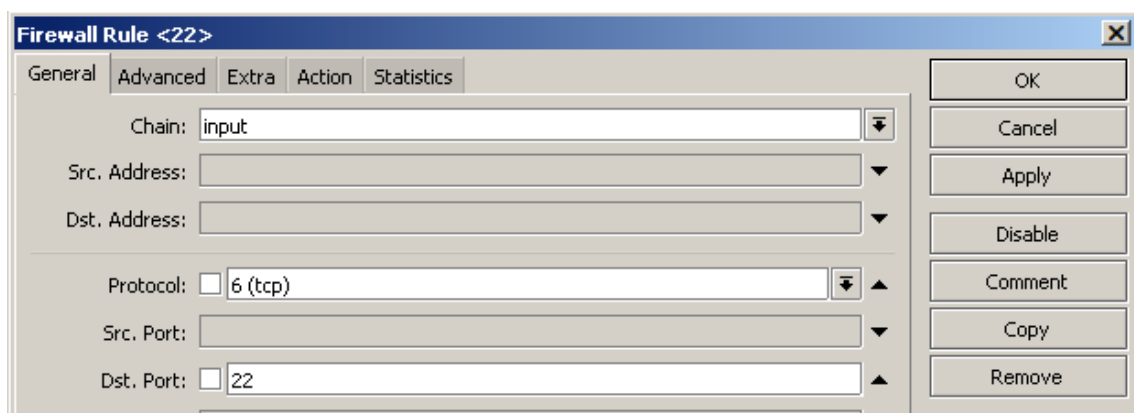
Route List

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DA	33.1.1.0/24	ether1 reachable	0		33.1.1.1
AS	33.1.2.0/24	172.16.1.2 reachable ether2	1		
AS	33.1.3.0/24	172.16.1.3 reachable ether2	1		
DA	172.16.1.0/24	ether2 reachable	0		172.16.1.1
DA	192.168.0.0/16	ether3 reachable	0		192.168.1.11

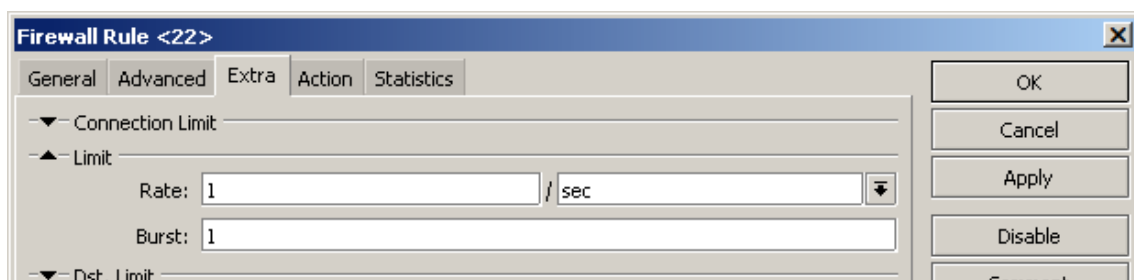
2. Configure el router para que detecte un ataque de fuerza bruta para acceder por SSH, y anote la dirección del ordenador que origina el ataque en una lista de direcciones IP. Básicamente consiste en que el atacante se conecta al servicio SSH (puerto TCP 22) y prueba distintos nombres de usuario y contraseñas. En este caso, las conexiones serán frecuentes. Para simular el ataque, lance el siguiente script desde línea de comandos:

```
$ awk 'BEGIN{for(i=0;i<1000;i++) print "nc <dir-ip-router>  
22 <a.sh" }' > a.sh; sh a.sh
```

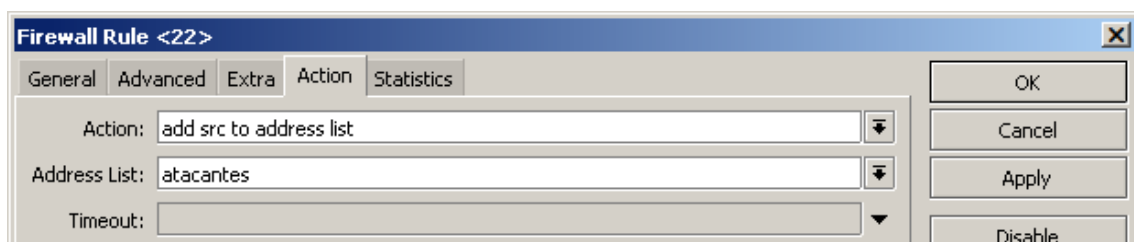
Creamos una nueva regla de cortafuegos desde el menú IP -> Firewall -> Botón +, para detectar todo el tráfico de entrada en la pestaña "General" seleccionamos "input" en el campo "Chain", como las conexiones SSH se realizan mediante TCP al puerto 22 seleccionamos en el campo "Protocol" el valor "6 (tcp)" y en "Dst. Port" el valor "22".



Indicamos un criterio adicional desde la pestaña "Extra", este será que se considerará ataque cuando el tipo de conexiones definidas en el paso anterior se repitan más de una vez por 1 ("Rate: 1/sec" y "Burst: 1").



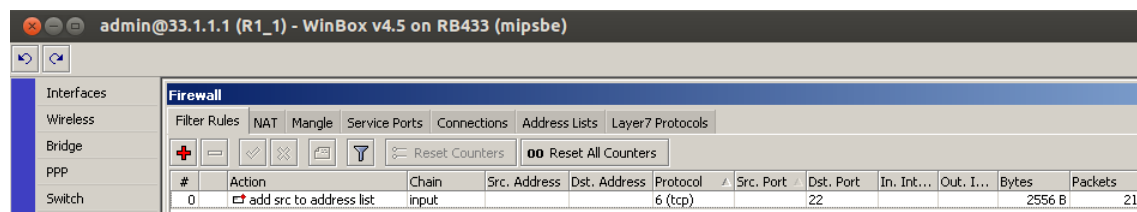
La acción a realizar cuando todo esto se cumpla es que la dirección IP desde la que se realiza dicho intento de ataque será añadida a una lista de direcciones que llamaremos "atacantes" ("Action: add src to address list" y "Address List: atacantes").



Para comprobar si la regla definida funciona correctamente, lanzamos el script del enunciado desde un terminal, lo que nos dará una salida similar a la siguiente. Nota: si lanzamos el script desde el ordenador que estamos conectados al router, precisamente al cumplir la regla, la conexión se cerrará y seremos “expulsados” del router.

```
SSH-1.99-OpenSSH_2.3.0_Mikrotik_v2.9
Protocol mismatch.
SSH-1.99-OpenSSH_2.3.0_Mikrotik_v2.9
Protocol mismatch.
SSH-1.99-OpenSSH_2.3.0_Mikrotik_v2.9
Protocol mismatch.
```

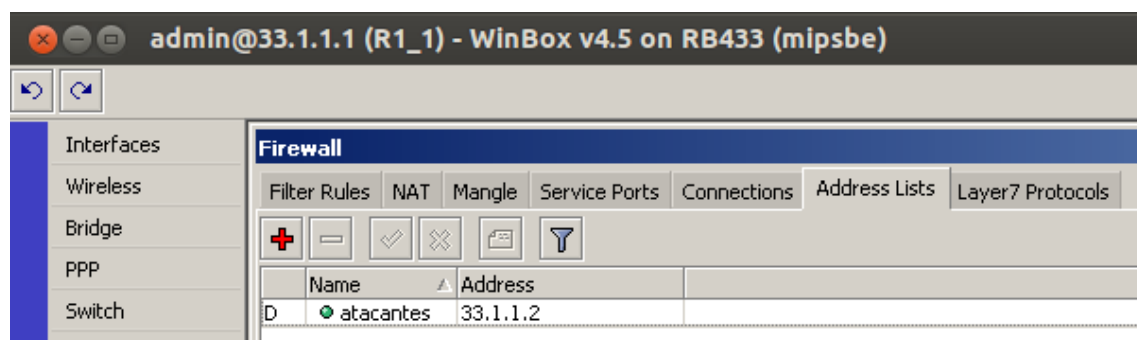
Vemos que la regla está funcionando, porque en su entrada correspondiente los campos “Bytes” y “Packets” están aumentando, lo que significa que el tráfico está siendo filtrado.



admin@33.1.1.1 (R1_1) - WinBox v4.5 on RB433 (mipsbe)

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets
0	add src to address list	input			6 (tcp)		22			2556 B	21

Además si nos metemos en la pestaña “Address Lists”, vemos que se ha creado una lista con el nombre “atacantes” con la IP desde la que estamos realizando el ataque “33.1.1.2”.

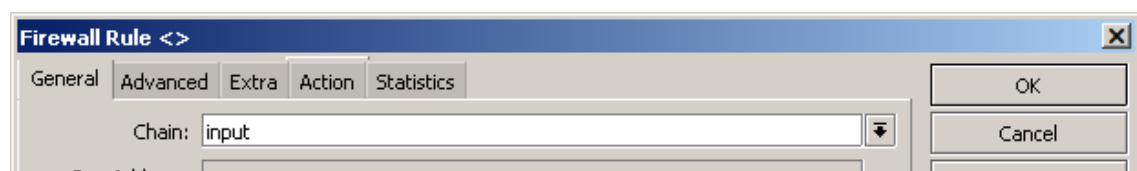


admin@33.1.1.1 (R1_1) - WinBox v4.5 on RB433 (mipsbe)

Name	Address
atacantes	33.1.1.2

3. Configure el router para que descarte los paquetes de la lista anterior.

Para que se descarte el tráfico concreto creamos una nueva regla que filtre todo el tráfico de entrada desde la pestaña “General” seleccionando para el campo “Chain” el valor “input”.



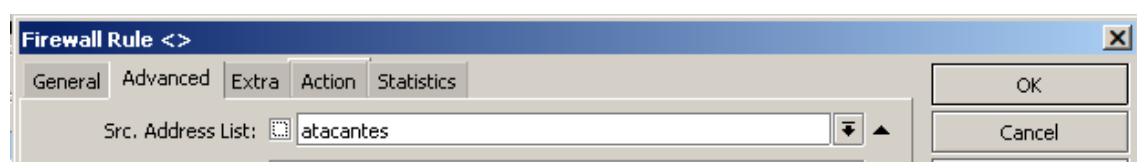
Firewall Rule <>

General Advanced Extra Action Statistics

Chain: input

OK Cancel

Para que el tráfico filtrado sea el de la lista anterior, desde la pestaña “Advanced” ponemos el nombre de la lista “atacantes” en el campo “Src. Address List”.



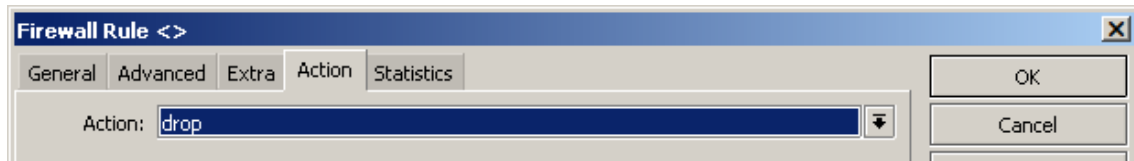
Firewall Rule <>

General Advanced Extra Action Statistics

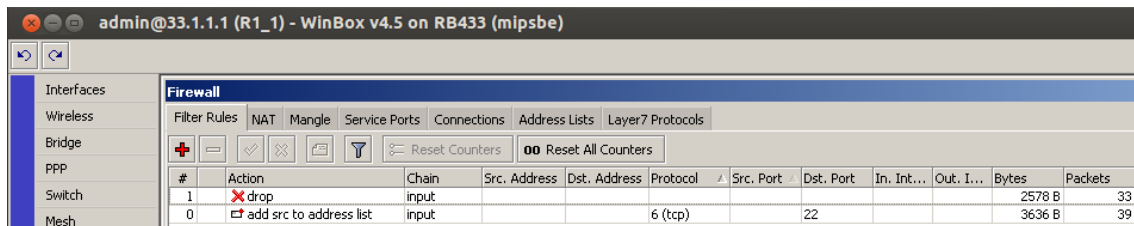
Src. Address List: atacantes

OK Cancel

E indicamos que la acción a realizar es tirar todos esos paquetes desde la pestaña “Action” seleccionando el valor “drop” en el campo “Action”.



Como con la regla anterior, vemos que se está aplicando porque los campos “Bytes” y “Packets” están aumentando su valor en la entrada de la regla que acabamos de definir.

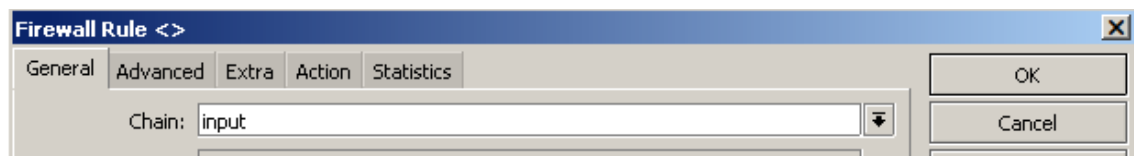


4. Configure el cortafuegos del router para que descarte el tráfico que contenga la cadena: “ZomBot”. Para generar el tráfico, puede usar la herramienta “netcat” con la siguiente sintaxis:

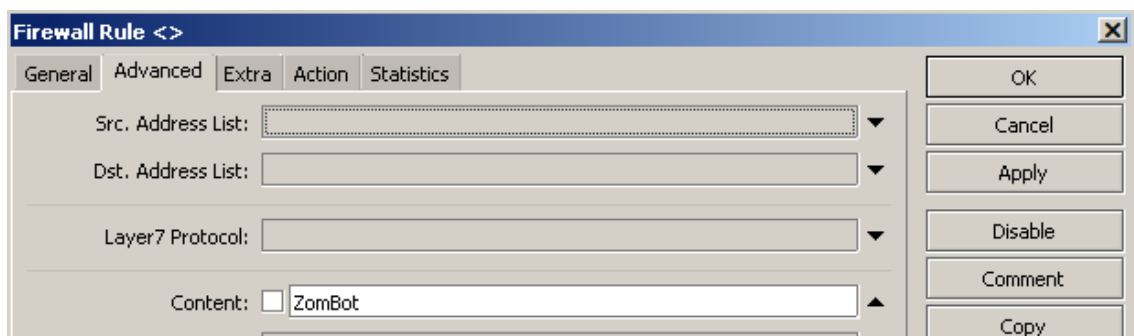
Parte servidor: \$ nc -l -p <puerto>

Parte cliente: \$ nc <ip-servidor> <puerto>

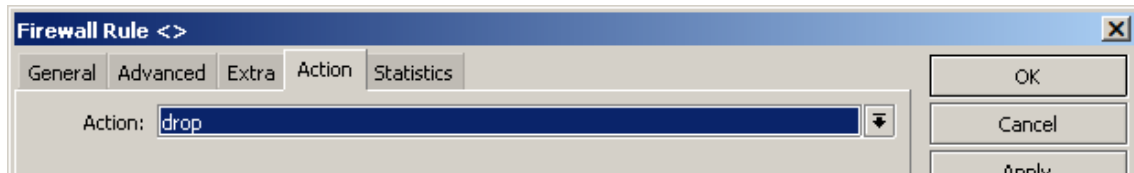
Para crear esta regla indicamos como en las otras que se debe aplicar sobre el tráfico de entrada: pestaña “General” -> campo “Chain” -> valor “input”.



Como queremos descartar todo el tráfico que contenga la cadena “ZomBot”, en la pestaña “Advanced” lo indicamos introduciendo el valor “ZomBot” en el campo “Content”.



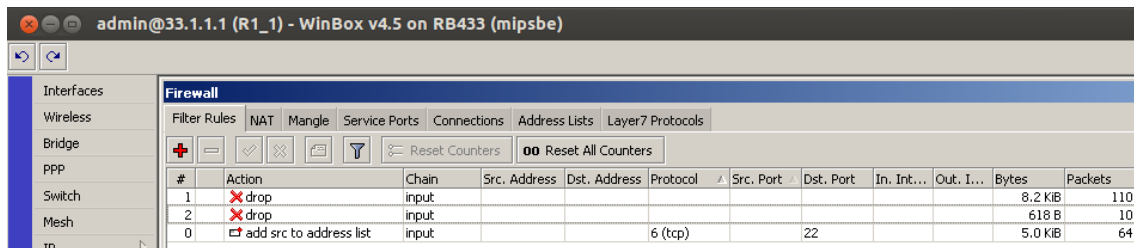
Volviendo a indicar que el tráfico que cumpla con dicha regla debe ser descartado: pestaña “Action”
-> campo “Action” -> valor “drop”.



Para comprobar que la regla funciona, desde un terminal usaremos el comando “nc” para conectarnos a nuestro router “33.1.1.1” usando el puerto “80”, una vez conectados introducimos varias veces la cadena “ZomBot” para comprobar si es filtrada.

```
administrador@ei141080:~$ nc 33.1.1.1 80
ZomBot
ZomBot
ZomBot
ZomBot
ZomBot
ZomBot
ZomBot
^C
```

Vemos que los campos “Bytes” y “Packets” correspondientes a la entrada de la regla que acabamos de crear están aumentando, por lo que los paquetes están siendo “tirados” por la regla que acabamos de crear.



#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Int...	Out. I...	Bytes	Packets
1	drop	input								8.2 KIB	110
2	drop	input								618 B	10
0	add src to address list	input			6 (tcp)		22			5.0 KIB	64